SMISHING Y OTRAS ESTAFAS EN LA RED

RECIÉN terminada la cuesta de enero es muy probable que no nos acordemos de la oleada de estafas en la red que hubo a finales de diciembre, pero fue un mes especialmente peligroso en este sentido. Está claro que el mal no descansa y menos en fechas en las que solemos estar preocupados por que llegue algún paquete a tiempo a casa o en las que hay muchos más gastos imprevistos en nuestra economía doméstica. Este es el escenario perfecto para el tipo de estafas que vamos a comentar en este artículo.

DEL *PHISHING* AL *SMISHING*

Bajo estos nombres tan raros se esconden estafas bien conocidas ya. La palabra *phishing* proviene de *fishing*: ir de pesca en inglés. Y es precisamente eso: utilizar un cebo (*bait* en inglés) para que piquemos el anzuelo y acabemos atrapados en la estafa.

El *phishing* se puede hacer de muchas maneras. La más común es mediante el correo electrónico por dos razones. La primera es que a los atacantes les resulta muy barato inundar nuestros buzones con correos fraudulentos. Enviar un correo electrónico con el remitente falso cuesta virtualmente cero y por eso les da igual que la tasa de éxito sea extremadamente baja. Con que una sola persona «pique», habrán merecido la pena los millones de correos que fueron borrados o filtrados por el resto de destinatarios. La segunda razón tiene que ver con las posibilidades que ofrecen los correos electrónicos escritos en HTML, el lenguaje de las páginas web. Estos correos pueden prepararse utilizando los logos, membretes, fondos, imágenes corporativas, etc. de la entidad que quiera suplantarse y solamente el ojo entrenado será capaz de darse cuenta del engaño.

Afortunadamente, nuestros proveedores de correo electrónico suelen tener filtros automáticos que nos bloquean muchos de estos ataques de *phishing* o nos añaden una alerta para que los leamos con cautela y no pulsemos en los enlaces que contienen. Por este motivo, los estafadores se han pasado al *smishing*, el *phishing* a través de mensajes SMS.

Falsear el remitente de un SMS o de una llamada telefónica es algo muy fácil de hacer y nos puede hacer creer que estamos ante información verídica de una fuente confiable.

Dado que muchos servicios de mensajería y de banca online combinan sus alertas mediante su app móvil, el correo electrónico y el SMS, estamos acostumbrados a recibir alertas de SMS para los eventos importantes como cuando ha habido un problema al entregar nuestro envío o cuando ha habido un movimiento anómalo de dinero en nuestra cuenta corriente. Si a esto le sumamos que muchas empresas envían sus SMS no desde un

número de teléfono sino desde un nombre de cuenta (por ejemplo, Correos en lugar de +34 689745543) y que algunos servidores internacionales permiten el envío de SMS indicando lo que quieras como remitente, tenemos el vector perfecto para que nos cuelen un enlace de *phishing* por SMS y que parezca legítimo.

Por supuesto, el enlace del SMS parecerá legítimo, algo como http://amazn.com/3453187, pero muy seguramente faltará alguna letra o alguna no será igual a la original (por ejemplo, un uno en lugar de una ele, o un cero en lugar de una o).

En esa página web nos pedirán todos nuestros datos para tratar de solucionar la incidencia y ahí es cuando habremos perdido. Quizá esos datos sensibles no se utilicen inmediatamente, quizá el robo de credenciales se aproveche mucho más tarde, pero ya estaremos en peligro hasta que no demos de baja todas las tarjetas u otros datos sensibles que hayamos facilitado a los estafadores.

ENGAÑOS EN LA IDENTIFICACIÓN DE LLAMADA

Otro tipo de estafas muy común últimamente es similar al *smishing*, pero usando una comprobación mediante una llamada de teléfono. Al igual que ocurre con los SMS, es posible realizar una llamada falseando el remitente de una llamada (técnicamente, se conoce como falsear el «caller ID») para que coincida exactamente con el teléfono oficial de nuestra operadora de telefonía, nuestro banco, o cualquier otra empresa de la que seamos clientes.

El falseo del «caller ID» es posible gracias a que hay muchos proveedores en Internet que ofrecen pasarelas de llamadas desde Internet a la red de telefonía móvil a tarifas muy baratas que normalmente no confirman que quien llama desde Internet es realmente quien dice ser. Algunas de estas pasarelas son denunciadas de cuando en cuando por no tener cuidado con esto, pero lo normal es que vuelvan a operar bajo otro dominio, así que es muy difícil evitar esta modificación del remitente.

La estafa suele tener un guion bastante recurrente. Inicialmente, nos llega un SMS de nuestro banco (falso) indicando que alguien se ha hecho con nuestras credenciales y ha retirado una cantidad de dinero de nuestra cuenta. Después, se nos pide que llamemos al teléfono de nuestro banco o que esperemos la llamada de una de sus operadoras. Al cabo de solo unos minutos, recibimos una llamada de la supuesta operadora del banco, desde el número de teléfono que aparece en la web de nuestro banco (falseado) y nos informa del supuesto incidente. Tras facilitarnos una explicación y parte de nuestros datos, nos informa de que el banco nos ha abierto una segunda cuenta corriente de manera gratuita y nos aconseja que movamos nuestros ahorros a esa segunda cuenta, facilitando por teléfono las claves necesarias para hacer esa transferencia.

Por supuesto, todo esto es mentira y lo que realmente estamos haciendo es transferir todo nuestro dinero a la cuenta de los estafadores. Para cuando nos demos cuenta, llamaremos al teléfono del banco y nos dirán que la llamada anterior no les consta y que hemos sido víctimas de una estafa.

CONSEJOS FINALES

Como podemos ver, falsear el remitente de un SMS o de una llamada telefónica es algo muy fácil de hacer y nos puede hacer creer que estamos ante información verídica de una fuente confiable.

> *Nunca proporcionar por teléfono datos sensibles como contraseñas, números de tarjeta de crédito u otras credenciales que permitan a un tercero acceder a nuestras cuentas.*

Lo más recomendable en estos casos es comprobar la información que nos llega por SMS o llamada desde la app oficial del banco o del servicio implicado. Es decir, llamar nosotros al banco o servicio y no esperar la llamada y, sobre todo, nunca proporcionar por teléfono datos sensibles como contraseñas, números de tarjeta de crédito u otras credenciales que permitan a un tercero acceder a nuestras cuentas.

Mantener la calma en una situación así es muy difícil, por lo que también es muy recomendable que sea alguien no implicado directamente (mejor un amigo o un familiar) quien nos aconseje sobre los pasos que dar y sobre la veracidad que puedan tener los mensajes y los enlaces recibidos. ¡Espero que todo esto os sirva para no morder el anzuelo!

PABLO GARAIZAR